(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 158 384 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
28.11.2001 Patentblatt 2001/48

(51) Int Cl.[7]: **G06F 1/00**, G06F 9/38, G07F 7/10

(21) Anmeldenummer: **00110838.0**

(22) Anmeldetag: **22.05.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(71) Anmelder: **Infineon Technologies AG**
81669 München (DE)

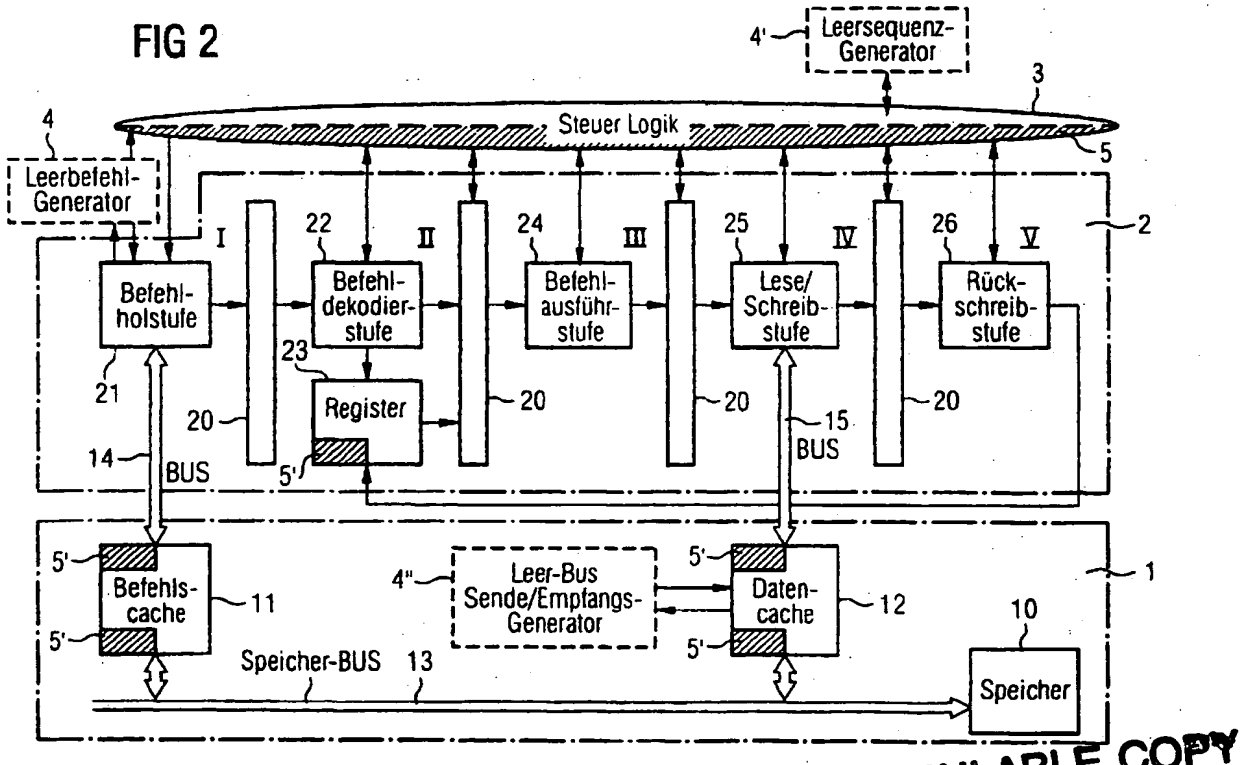
(72) Erfinder: **May, Christian**
81677 München (DE)

(74) Vertreter: **Kindermann, Peter, Dipl.-Ing. et al**
Patentanwalt,
Postfach 1330
85627 Grasbrunn (DE)

(54) Sicherheits-Datenverarbeitungseinheit sowie dazugehöriges Verfahren

(57) Die Erfindung betrifft eine Sicherheits-Datenverarbeitungseinheit sowie ein dazugehöriges Verfahren mit einem Daten/Programmbefehlsspeicher (1) zum Speichern von Daten/Programmbefehlen, einer Befehlsleitung (2) mit einer Vielzahl von Funktionsstufen (I bis V) zum Verarbeiten der Daten/Programmbefehle, und einer Steuereinheit (3) zum Steuern der Funktionsstufen (I bis V). Ein Leerfunktionsgenerator (4, 4', 4") erzeugt hierbei zufällig Leerfunktionen in der Datenverarbeitungseinheit, wodurch ein Lauschangriff mittels Analyse von Leck-Informationen wesentlich erschwert bzw. verhindert wird.

FIG 2



EP 1 158 384 A1

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Sicherheits-Datenverarbeitungseinheit sowie ein dazugehöriges Verfahren und insbesondere auf eine Sicherheits-Datenverarbeitungseinheit sowie ein dazugehöriges Verfahren, welches eine kryptographische Verschlüsselung und/oder Zugangsberechtigung vor unerlaubten externen Lauschangriffen schützt.

[0002] Durch die zunehmende Verbreitung von beispielsweise kryptographischen Systemen zur elektronischen Verschlüsselung von sicherheitsrelevanten Daten und/oder zur elektronischen Zugangsberechtigung in sicherheitsrelevanten Bereichen besteht zunehmend der Bedarf nach Sicherheits-Datenverarbeitungseinheiten, die insbesondere gegenüber externen Angriffen wie z.B. Lauschangriffen geschützt sind.

[0003] Die meisten kryptographischen Systeme benötigen eine sichere Behandlung der bei der kryptographischen Verarbeitung verwendeten Schlüssel. In Sicherheitssystemen mit sogenannten öffentlichen Schlüsseln (public-keys) müssen die dazugehörigen privaten Schlüssel (private-keys) derart geschützt sein, dass mögliche Angreifer den oder die Schlüssel auf keinen Fall lesen bzw. entziffern können, da ansonsten beispielsweise digitale Signaturen gefälscht, Daten modifiziert und geheime Informationen dechiffriert werden können.

[0004] Im wesentlichen unterscheidet man hierbei zwischen symmetrischen und asymmetrischen Algorithmen bzw. kryptographischen Protokollen, mit deren Hilfe ein unerwünschter Datenangriff auf vertrauliche oder geheime Daten verhindert werden kann.

[0005] Beispielsweise müssen kryptographische Kodiervorrichtungen zur Realisierung einer Verschlüsselung und/oder einer Zugangsberechtigung ihre geheimen Schlüssel selbst dann sicher schützen, wenn sie sich in einer angreifbaren Umgebung befinden. Als derartige kryptographische Kodiervorrichtungen mit dazugehörigen Datenverarbeitungseinheiten sind beispielsweise sogenannte Chipkarten, Smartcards, oder sicherheitsrelevante Module bekannt, die beispielsweise bei Geldautomaten, KFZ-Wegfahrsperren, usw. eine gesicherte Zugangsberechtigung und/oder eine gesicherte Verschlüsselung von Daten ermöglichen.

[0006] Figur 1 zeigt eine schematische Darstellung einer derartigen Kodiervorrichtung bzw. eines Zustandsautomaten ZA zur Realisierung beispielsweise einer kryptographischen Verschlüsselung und/oder Zugangsberechtigung, die im wesentlichen aus einer kryptographischen Datenverarbeitungseinheit DV besteht und eine Eingabe bzw. eingegebene Daten beispielsweise unter Verwendung eines geheimen Schlüssels PK (private key) kryptographisch verarbeitet. Die von der Datenverarbeitungseinheit DV verarbeiteten Daten werden anschließend an einer Ausgabe ausgegeben, wodurch die kryptographische Verschlüsselung und/oder eine gesicherte Zugangsberechtigung realisiert wird.

[0007] Der in Figur 1 dargestellte Zustandsautomat ZA wird beispielsweise als Chipkarte, Smartcard, gesicherte Mikroprozessoreinheit oder dergleichen realisiert. Demzufolge verwendet die kryptographische Kodiervorrichtung ZA den geheimen Schlüssel PK zum Verarbeiten von eingegebenen Informationen und zum Ausgeben bzw. Erzeugen von Informationen, wobei die kryptographischen Algorithmen bzw. die Protokolle üblicherweise derart entworfen sind, dass ein Angriff auf die zu verschlüsselnden oder geheimen Daten an der Eingabe- oder Ausgabeschnittstelle abgewehrt werden kann. Es hat sich jedoch herausgestellt, dass wesentlich wirkungsvollere externe Angriffe auf kryptographische Datenverarbeitungseinheiten bzw. die darin abgearbeiteten Kodierverfahren und deren geheime Schlüssel auch über sogenannte Leck-Informationen erfolgen können. Gemäß Figur 1 sind dies beispielsweise ein Stromverbrauch, eine elektromagnetische Abstrahlung oder dergleichen, die bei der kryptographischen Datenverarbeitung Rückschlüsse über die verwendeten geheimen Schlüssel bzw. das verwendete kryptographische Verfahren ermöglichen.

[0008] Die vorliegende Erfindung beschäftigt sich hierbei insbesondere mit einem Angriff über eine sogenannte statistische Analyse von physikalischen Signalen wie beispielsweise einem Stromprofil der Datenverarbeitungseinheit DV. Bei der Analyse eines Stromprofils der Datenverarbeitungseinheit DV wird hierbei der Umstand ausgenutzt, dass integrierte Schaltungen aus einer Vielzahl von einzelnen Transistoren bestehen, die im wesentlichen als spannungsgesteuerte Schalter arbeiten. Hierbei fließt beispielsweise Strom über ein Transistorsubstrat, sobald Ladungen an einem Gate angelegt oder entfernt werden. Dieser Strom liefert wiederum Ladungen an die Gates von weiteren Transistoren, wodurch wiederum weitere Verdrahtungsabschnitte oder Lasten geschaltet werden. Ein derartiges Schaltverhalten, das insbesondere auch beim Abarbeiten von kryptographischen Algorithmen durchgeführt wird, ist daher über die Stromversorgung der Datenverarbeitungseinheit DV bzw. des Zustandsautomaten ZA meßbar und ermöglicht Angreifern beispielsweise das Lesen des geheimen Schlüssels PK.

[0009] Die bekanntesten Stromprofilanalysen sind hierbei die einfache Stromprofilanalyse (simple power analysis, SPA), die differentielle Stromprofilanalyse (differential power analysis, DPA) und die differentielle Stromprofilanalyse höherer Ordnung (high-order differential power analysis, HO-DPA). Während die einfache Stromprofilanalyse SPA im wesentlichen eine visuelle Überwachung der Schwankungen im Stromverbrauch berücksichtigt, verwenden Angriffe mittels der differentiellen Stromprofilanalyse DPA statistische Analyseverfahren sowie Fehlerkorrekturverfahren zum Extrahieren von Informationen, die mit geheimen Schlüsseln korreliert sind. Differentielle Stromprofilanalysen höherer Ordnung (HO-DPA) verbessern die Möglichkeiten eines Angriffs zum Extrahieren von geheimen Schlüsseln mit-

tels eines meßbaren Stromverbrauchs, wobei jedoch die differentielle Stromprofilanalyse in den meisten Fällen zum "Abhören" der verarbeiteten Daten bereits ausreicht.

[0010] Zur Verhinderung derartiger Angriffe auf Datenverarbeitungseinheiten in sicherheitsrelevanten Einsatzgebieten ist beispielsweise aus der Druckschrift WO 99/35782 ein kryptographisches Verfahren und eine kryptographische Vorrichtung bekannt, mittels derer die genannten Stromprofilanalysen unwirksam werden. Im wesentlichen ist hierbei ein Verfahren und eine Vorrichtung beschrieben, bei dem sich durch ständiges Ändern der für die kryptographische Datenverarbeitung wesentlichen Schritte die für einen Angreifer lesbare Leck-Information sozusagen "selbstheilend" auslöscht. Dadurch werden insbesondere statistische Auswertungen verhindert und ein Angriff über beispielsweise den Stromverbrauch einer Datenverarbeitungseinheit DV bzw. über elektromagnetische Abstrahlung zuverlässig verhindert.

[0011] Nachteilig bei einer derartigen Realisierung eines Angriffsschutzes ist jedoch die Tatsache, dass schwerwiegende Eingriffe in die kryptographische Software des Systems bzw. der dazugehörigen Datenverarbeitungseinheit vorgenommen werden müssen. Genauer gesagt kann ein derartiger Schutz nur in Kenntnis der jeweiligen kryptographischen Algorithmen bzw. Protokolle durchgeführt werden, die entsprechend abgeändert werden oder sich gegebenenfalls selbständig abändern. Ein derartiger Eingriff in die unmittelbare Software der kryptographischen Datenverarbeitung erfordert jedoch einen außerordentlich hohen Aufwand, ist darüber hinaus nur von Experten zu realisieren und von jeweiligen Benutzern (Kunden) oftmals nicht erwünscht, da ein derartiger Hersteller wiederum die Kenntnis zum Brechen des Schutzes besitzt.

[0012] Als weitere Möglichkeit zur Verhinderung derartiger Angriffe können ferner sogenannte zusätzliche Stromprofilgeneratoren verwendet werden, die einem für die Stromprofilanalyse nutzbaren Stromprofil ein Störstromprofil überlagern und somit zumindest eine einfache Stromprofilanalyse verhindern. Ein Schutz gegenüber differentieller Stromprofilanalyse bzw. einer Stromprofilanalyse höherer Ordnung ist jedoch dadurch nicht zu erreichen.

[0013] Der Erfindung liegt daher die Aufgabe zugrunde, eine Sicherheits-Datenverarbeitungseinheit zu schaffen, die ohne Modifikation von kryptographischen Programmen externe Lauschangriffe zuverlässig verhindert.

[0014] Erfindungsgemäß wird diese Aufgabe hinsichtlich der Sicherheits-Datenverarbeitungseinheit durch die Merkmale des Patentanspruchs 1 und hinsichtlich des Verfahrens durch die Maßnahme des Patentanspruchs 11 gelöst.

[0015] Insbesondere durch die Verwendung eines Leerfunktionsgenerators zum Erzeugen von Leerfunktionen in der Datenverarbeitungseinheit und erforderlichenfalls eines Leerfunktionskompensators zum Kompensieren der erzeugten Leerfunktionen in der Datenverarbeitungseinheit erhält man eine Desynchronisation des Instruktions- bzw. Befehlsablaufs für unterschiedliche Anfangsdaten eines jeweiligen kryptographischen Entschlüsselungsprozesses. Ein Auffinden von Triggerpunkten in den Stromprofilen der Datenverarbeitungseinheit kann dadurch zuverlässig verhindert werden, wodurch eine Stromprofilanalyse mittels Resynchronisation von Datensätzen in ihrem zeitlichen Verlauf erschwert bzw. verhindert wird.

[0016] Vorzugsweise werden durch den Leerfunktionskompensator Schreibvorgänge auf von Programmen nutzbare Register/Speicherstellen verhindert, wodurch sich eine besonders einfache Kompensation der erzeugten Leerfunktionen ergibt und keine Beeinflussung eines effektiven Programmflusses verursacht wird.

[0017] Zur Verbesserung eines Schutzes gegen externe Angriffe können vom Leerfunktionsgenerator Leerbefehle in Form von erlaubten Programmbefehlen erzeugt werden. Ein Erfassen dieser Leerbefehle ist hierbei besonders schwierig.

[0018] Alternativ oder zusätzlich kann der Leerfunktionsgenerator einen Leersequenzgenerator aufweisen, welcher zusätzlich zu benötigten Funktionsstufen nicht genutzte Funktionsstufen in einer Befehlsleitung aktiviert. Auf diese Weise können über Aktivierungsleckinformationen (Ströme) von jeweiligen Funktionsstufen keine Rückschlüsse auf einen jeweils verarbeiteten Befehl geschlossen werden.

[0019] In ähnlicher Weise kann zusätzlich oder alternativ der Leerfunktionsgenerator einen Leer-Lese/Schreib-Generator zum Erzeugen von zusätzlichen Lese/Schreib-Vorgängen auf schnelle Daten-/Programmbefehls-Zwischenspeicher aufweisen, wodurch besonders einfach zu erfassende Leckinformationen eines Speicherbusses unbrauchbar gemacht werden können.

[0020] Eine Zufallssteuerung zum zufälligen Ansteuern des Leerfunktionsgenerator kann hierbei sowohl eine echte Zufälligkeit als auch eine Pseudozufälligkeit (deterministisch) aufweisen und wahlweise ein- oder ausschaltbar sein.

[0021] In den weiteren Unteransprüchen sind weitere vorteilhafte Ausgestaltungen der Erfindung gekennzeichnet.

[0022] Die Erfindung wird nachstehend anhand von Ausführungsbeispielen unter Bezugnahme auf die Zeichnung näher beschrieben.

[0023] Es zeigen:

Figur 1 eine schematische Darstellung zur Veranschaulichung eines Angriffs über Leck-Informationsanalyse gemäß dem Stand der Technik; und

Figur 2 eine vereinfachte Blockdarstellung eines Teils der erfindungsgemäßen Sicherheits-Datenverarbeitungseinheit.

[0024] Figur 2 zeigt eine vereinfachte Blockdarstellung eines Teils einer Sicherheits-Datenverarbeitungseinheit DV gemäß der vorliegenden Erfindung, wobei zur Vereinfachung eine Vielzahl von weiteren wesentlichen Teilen der Sicherheits-Datenverarbeitungseinheit nicht dargestellt sind.

[0025] Der in Figur 2 dargestellte Teil der erfindungsgemäßen Sicherheits-Datenverarbeitungseinheit besitzt im wesentlichen einen Daten-/Programmbefehlsspeicher 1 zum Speichern von Daten und Programmbefehlen. Der Daten-/Programmbefehlsspeicher 1 besitzt gemäß Figur 2 einen schnellen Programmbefehl-Zwischenspeicher bzw. Befehlscache 11 sowie einen schnellen Daten-Zwischenspeicher bzw. -cache 12 die über einen Speicherbus 13 mit einem herkömmlichen (langsamer Zugriff) Speicher 10 in Verbindung stehen.

[0026] Ferner besitzt die Sicherheits-Datenverarbeitungseinheit zumindest eine Befehlsleitung bzw. Pipeline 2 mit einer Vielzahl von Funktionsstufen bzw. Pipeline-Stufen I bis V zum Verarbeiten der Daten/Programmbefehle. Die schnellen Daten-/Programmbefehls-Zwischenspeicher 11 und 12 dienen demzufolge als Busanpassung zwischen der Befehlsleitung 2 und dem Speicher 10. Gemäß Figur 2 besitzt die Befehlsleitung 2 eine Befehlsholstufe 21, mittels der über einen Befehlsbus 14 und den schnellen Programmbefehlsspeicher 11 Programmbefehle nacheinander aus dem Speicher 10 geholt werden. Anschließend werden die Programmbefehle über einen Zwischenspeicher 20 einer Befehlsdekodierstufe 22 zugeführt, wobei gleichzeitig eine Steuereinheit 3 dazugehörige Steuerinformationen erhält. Die Steuereinheit 3 dient im wesentlichen einer Steuerung der Vielzahl von Funktionsstufen I bis V der Befehlsleitung 2 und steuert eine Abarbeitung des geholten Programmbefehls über die weiteren Funktionsstufen.

[0027] Beispielsweise kann die Steuereinheit 3 eine Addition von Registern 23 aus der Funktionsstufe II über einen weiteren Zwischenspeicher 20 in einer nachfolgenden Befehlausführstufe 24 anordnen. Nachdem ein Ergebnis dieser Addition über einen weiteren Zwischenspeicher 20 an eine Lese/Schreistufe 25 weitergereicht wurde, kann die Steuereinheit 3 ein Laden eines Wertes an einer Adresse des berechneten Ergebnisses aus dem Speicher 10 über eine Datenbus 15 und den schnellen Daten-Zwischenspeicher 12 anweisen. Für bestimmte Funktionen kann ferner dieses Ergebnis zur erneuten Verarbeitung über einen weiteren Zwischenspeicher 20 und eine Rückschreibstufe 26 an das Register 23 der Funktionsstufe II zurückgeschrieben werden. Die Zwischenspeicher bzw. -register 20 dienen hierbei einer Entkopplung der jeweiligen Verarbeitungs- bzw. Funktionsstufen I bis V, wodurch eine gleichzeitige Abarbeitung von Daten/Programmbefehlen in den jeweiligen Stufen ermöglicht wird.

[0028] Da sowohl ein Programmbefehl und eine Datenverarbeitung in jeder dieser Funktionsstufen als auch ein Daten-/Programmbefehltransport über einen der Busse 13, 14 und 15 zu auswertbaren charakteristischen (optischen, elektrischen, elektromagnetischen) Lecksignalen führt, können diese Signale mittels der eingangs beschriebenen SPA- und DPA-Angriffe erfasst und analysiert werden. Ein DPA-Angriff basiert hierbei im wesentlichen auf einer zeitlichen Korrelationsanalyse zwischen ablaufendem Programmcode und dem dazugehörigen Profil des Lecksignals, wodurch auf verarbeitete Datengeheimnisse rückgeschlossen werden kann. Die Korrelation wird hierbei über viele Messungen ermittelt.

[0029] Zur Verhinderung eines derartigen DPA-Angriffs bzw. einer Korrelationsanalyse besitzt die erfindungsgemäße Sicherheits-Datenverarbeitungseinheit einen Leerfunktionsgenerator zum Erzeugen von Leerfunktionen und erforderlichenfalls einen Leerfunktionskompensator zum nachfolgenden Kompensieren der erzeugten Leerfunktionen in der Datenverarbeitungseinheit.

Erstes Ausführungsbeispiel

[0030] Gemäß einem ersten Ausführungsbeispiel wird der Leerfunktionsgenerator durch einen Leerbefehlgenerator 4 realisiert, der Leerbefehle erzeugt und unmittelbar in die Befehlholstufe 21 einschleust. Im einfachsten Fall können hierbei sogenannten NOP-Befehle (no operation) oder "wait-state"-Befehle (Warten) eingefügt werden, wobei jedoch das Problem auftritt, dass derartige Befehle aufgrund ihres charakteristischen Lecksignals leicht zu erkennen und herauszufiltern sind. Vorzugsweise werden daher erlaubte Programmbefehle vom Leerbefehlgenerator 4 erzeugt, wie sie auch im abgearbeiteten Programmcode vorkommen können. Der Leerbefehlgenerator 4 erzeugt diese Dummy- bzw. Leerbefehle mittels eines (nicht dargestellten) Zufallsgenerators oder deterministisch. Ferner kann das Erzeugen dieser Leerbefehle durch ein Zwischenspeichern von tatsächlich abzuarbeitenden Programmbefehlen aus der Befehlsholstufe 21 erfolgen, die zu einem späteren Zeitpunkt zufällig oder deterministisch an der Befehlholstufe 21 wieder eingeschleust werden.

[0031] Ein derart erzeugter Leerbefehl wird daher von der Befehlsleitung 2 bzw. der Datenverarbeitungseinheit in gleicher Weise abgearbeitet wie ein erlaubter Programmbefehl. Er erzeugt demzufolge auch ähnliche Lecksignale wie die Programmbefehle, wodurch eine Korrelationsanalyse zuverlässig verhindert wird. Um jedoch einen Einfluss der eingefügten Leerbefehle auf den eigentliche Programmabarbeitung zu verhindern, informiert der Leerbefehlgenerator 4 die Steuereinheit 3 darüber, dass die erzeugten Leerfunktionen erforderlichenfalls zu kompensieren sind. Genauer gesagt werden durch einen in der Steuereinheit 3 befindlichen Leerfunktionskompensator 5 Schreibvorgänge auf von Programmen nutzbare Register/Speicherstellen für jeden Leerbefehl verhindert. Eine Beeinflussung der Ergebnisse der gewünschten Programmverarbeitung

durch die eingefügten Leerbefehle wird dadurch zuverlässig ausgeschlossen.

[0032] Dieses Verhindern von Schreibvorgängen auf von Programmen nutzbare Register/Speicherstellen kann hierbei unmittelbar von dem Leerfunktionskompensator 5 durchgeführt werden, indem die jeweiligen Daten/Programmbefehle unmittelbar vor dem Einschreiben in ein Register/Speicherstelle verworfen werden. Alternativ kann dieses Verhindern von Schreibvorgängen auf von Programmen nutzbare Register/Speicherstellen durch zusätzliche nicht nutzbare Register/Speicherstellen 5' erfolgen, die im Falle von Leerbefehlen beschrieben werden, jedoch von der gewünschten Programmverarbeitung nicht genutzt bzw. ausgewertet werden. Diese nicht nutzbaren Register/Speicherstellen 5' befinden sich beispielsweise im Register 23 und in den schnellen Daten/Programmbefehl-Zwischenspeichern 11 und 12. Sie sind jedoch nicht darauf beschränkt und können sich auch an anderer Stelle in der Sicherheits-Datenverarbeitungseinheit befinden.

[0033] Eine Kompensation ist jedoch bei gewissen Befehlen (z.B. NOP) der mit einem den Programmzustand nicht ändern nicht erforderlich. Insbesondere bei einer Leerfunktion die eine Addition mit dem Wert "0" darstellt ist eine Kompensation nicht erforderlich, da trotz Erzeugung eines "Additions"-Leersignals eine Programmbeeinflussung nicht stattfindet und ein herausfiltern der Leerfunktion sogar schwierig

Zweites Ausführungsbeispiel

[0034] Gemäß einem zweiten Ausführungsbeispiel wird der Leerfunktionsgenerator durch einen Leersequenzgenerator 4' realisiert der zumindest eine zusätzliche nicht benötigte Funktionsstufe der Befehlsleitung 2 aktiviert. Der nachfolgend beschriebene Leersequenzgenerator 4' kann hierbei sowohl alleine als auch in Kombination mit dem vorstehend beschriebenen Leerbefehlgenerator 4 betrieben werden. Zur Vermeidung von Wiederholungen wird hierbei hinsichtlich der Funktionsweise des Leerfunktionskompensators 5 und 5' auf die Beschreibung des ersten Ausführungsbeispiels verwiesen. Eine Kompensation einer Leerfunktion ist nicht generell erforderlich (z.B. kann in der Befehlsausführstufe statt dem alleinigen weiterreichen eines Datums eine Addition mit 0 als Leerbefehl ausgeführt werden und das Ergebnis zur nächsten Stufe weitergereicht werden.

[0035] Gemäß dem vorliegenden zweiten Ausführungsbeispiel kann es bei der Abarbeitung von Befehlen des gewünschten Programmcodes in der Befehlsleitung 2 dazu kommen, dass Teilstufen der Befehlsleitung 2 für einen vorbestimmten Befehl nicht benötigt werden. Beispielsweise kann ein Ergebnis einer Operation in der Lese-/Schreibstufe 25 in den schnellen Daten-Zwischenspeicher 12 oder alternativ über die Rückschreibstufe 26 in das Register 23 eingeschrieben werden. Damit zwei derartig unterschiedliche Befehle mittels DPA-Angriff nicht unterschieden werden können, werden durch den Leersequenzgenerator 4' auch solche Funktionsstufen aktiviert, die für die eigentliche Programmverarbeitung nicht notwendig sind. Es entstehen somit für alle Programmbefehle gleiche Aktivierungs-Lecksignale. Alternativ können jedoch auch nur einzelne nicht benutzte Funktionsstufen einer jeweiligen Befehlsleitung 2 selektiv aktiviert werden, wodurch sich eine weitere Verbesserung einer Dekorrelation und/oder Dekohärenz ergibt.

[0036] Eine Ansteuerung des Leersequenzgenerators 4' kann hierbei wiederum rein zufällig oder deterministisch erfolgen. Die Steuerung der Befehlsleitung 2 erfolgt vorzugsweise durch eine Steuerleitung der Steuereinheit 3 oder durch zusätzlich Informationen, die auf den Bussen übertragen werden.

Drittes Ausführungsbeispiel

[0037] Gemäß einem dritten Ausführungsbeispiel wird der Leerfunktionsgenerator durch einen Leer-Bus Sende/Empfangsgenerator 4" realisiert, der zusätzliche Lese/Sendevorgänge auf die Bus-Interface Funktionsblöcke wie beispielsweise die schnellen Daten-/Programmbefehl-Zwischenspeicher 11 und 12 erzeugt. Der nachfolgend beschriebene Leer-Bus Sende/Empfangsgenerator 4" kann hierbei sowohl alleine als auch in Kombination mit dem vorstehend beschriebenen Leerbefehlgenerator 4 und Leersequenzgenerator 4' betrieben werden. Zur Vermeidung von Wiederholungen wird hierbei hinsichtlich der Funktionsweise des Leerfunktionskompensators 5 und 5' auf die Beschreibung des ersten Ausführungsbeispiels verwiesen.

[0038] Eine Kompensation eines Leer-Bus Sende-Befehls ist nicht erforderlich, wenn dieser Sende-Befehl von allen angeschlossenen Bus-Interface Funktionsblöcken wie z.B. Speicher 10 oder Lese/Schreibstufe 25 ignoriert wird.

[0039] Gemäß dem vorliegenden dritten Ausführungsbeispiel muss ein Sende/Empfangsvorgang bzw. Lese/Schreibvorgang eines Datums oder Programmbefehls nicht notwendigerweise zu einem Lese/Schreibvorgang im Speicher 10 führen, sondern kann durch das Lesen/Schreiben eines entsprechenden Elements beispielsweise im schnellen Daten-Zwischenspeicher 12 abgeschlossen sein. Der Lese/Schreibvorgang auf den Speicher 10 vom schnellen Daten-Zwischenspeicher 12 wird nur bei Bedarf ausgeführt, wenn ein Datum noch nicht in den schnellen Daten-Zwischenspeicher 12 geladen ist oder daraus entfernt wird. Um die Aktivität von Bus-Interface Funktionsblöcken mittels DPA-Angriffen wie etwa die zu erfassende Speicherzugriffe insbesondere zwischen Speicher 10 und schnellem Daten-Zwischenspeicher 12 zu verschleiern, können durch den Leer-Bus Sende/Empfangsgenerator 4" zusätzliche Leer-Lese/Schreibvorgänge bzw. Sende/Empfangsvorgänge erzeugt werden.

[0040] Wie beim ersten Ausführungsbeispiel kann

hierbei zur Vermeidung einer Beeinflussung des eigentlichen Programms entweder ein Buszugriff unmittelbar vor dem physikalischen Schreiben des Register/Speicherstelle abgebrochen oder in ein nicht nutzbares Register/Speicherstelle 5' geschrieben werden. Die Steuerung erfolgt wiederum durch eine Steuerleitung der Steuereinheit 3 oder durch zusätzliche Informationen, die auf den Bussen übertragen werden.

[0041] Die Erfindung wurde vorstehend anhand eines Leerfunktionsgenerators beschrieben, der Leerfunktionen in einer Datenverarbeitungseinheit mit einer 5-stufigen Befehlsleitung erzeugt. Die Datenverarbeitungseinheit kann jedoch auch eine Vielzahl von Befehlsleitungen oder eine andersartige Befehlsleitung aufweisen. Ferner wurde der Sende/Empfangsgenerator in Kombination mit schnellen Daten/Programmbefehl-Zwischenspeichern beschrieben, er kann jedoch auch mit Zwischenspeichern für Steuersignale und -befehle betrieben werden.

Patentansprüche

1. Sicherheits- Datenverarbeitungseinheit mit

   einem Daten-/Programmbefehlsspeicher (1) zum Speichern von Daten/Programmbefehlen; zumindest einer Befehlsleitung (2) mit einer Vielzahl von Funktionsstufen (21-26) zum Verarbeiten der Daten/Programmbefehle; und einer Steuereinheit (3) zum Steuern der Vielzahl von Funktionsstufen (21-26) der Befehlsleitung (2),

   gekennzeichnet durch
   einen Leerfunktionsgenerator (4, 4', 4") zum Erzeugen von Leerfunktionen in der Datenverarbeitungseinheit.

2. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 1, **dadurch gekennzeichnet, dass** die erzeugten Leerfunktionen inhärent keine Auswirkung auf einen gewünschten Programmablauf haben.

3. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 1, **gekennzeichnet durch**
   einen Leerfunktionskompensator (5, 5') zum Kompensieren von erzeugten Leerfunktionen in der Datenverarbeitungseinheit, die inhärent eine Auswirkung auf einen gewünschten Programmablauf haben.

4. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 3, **dadurch gekennzeichnet, dass** der Leerfunktionskompensator (5, 5') Schreibvorgänge auf von Programmen nutzbare Register/Speicherstellen verhindert.

5. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 4,
   dadurch gekennzeichnet, dass der Leerfunktionskompensator (5) einen Teil der Steuereinheit (3) darstellt und für Leerfunktionen Schreibvorgänge in der Datenverarbeitungseinheit unmittelbar verhindert.

6. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 4, **dadurch gekennzeichnet, dass** der Leerfunktionskompensator (5, 5') einen Teil der Steuereinheit (3) darstellt und von Programmen nicht nutzbare Register/Speicherstellen (5') aufweist, wobei für Leerfunktionen Schreibvorgänge in der Datenverarbeitungseinheit auf die nicht nutzbaren Register/Speicherstellen (5') erfolgen.

7. Sicherheits-Datenverarbeitungseinheit nach einem der Patentansprüche 1 bis 6,
   dadurch gekennzeichnet, dass der Leerfunktionsgenerator einen Leerbefehlgenerator (4) zum Erzeugen von Leerbefehlen aufweist.

8. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 7, **dadurch gekennzeichnet, dass** der Leerbefehlgenerator (4) einen erlaubten Programmbefehl erzeugt.

9. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 8,
   dadurch gekennzeichnet, dass der Leerbefehlgenerator (4) den erlaubten Programmbefehl aus tatsächlich verarbeiteten Programmbefehlen ableitet.

10. Sicherheits-Datenverarbeitungseinheit nach einem der Patentansprüche 1 bis 9,
    dadurch gekennzeichnet, dass der Leerfunktionsgenerator einen Leersequenzgenerator (4') zum Aktivieren von zumindest einer zusätzlichen Funktionsstufe (I - V) der Befehlsleitung (2) aufweist.

11. Sicherheits-Datenverarbeitungseinheit nach einem der Patentansprüche 1 bis 10,
    dadurch gekennzeichnet, dass die Datenverarbeitungseinheit Bus-Interface Funktionsblöcke (11, 12) zum Verbinden von unterschiedlichen Bussystemen (13, 14, 15) äufweist, und
    der Leerfunktionsgenerator einen Leer-Bus Sende/Empfangs - Generator (4") zum Erzeugen von zusätzlichen Sende/Empfangs - Vorgängen auf die Bus-Interface Funktionsblöcke (11, 12) aufweist.

12. Sicherheits-Datenverarbeitungseinheit nach Patentanspruch 11, **dadurch gekennzeichnet, dass** die Bus-Interface Funktionsblöcke schnelle Daten-/Programmbefehls-Zwischenspeicher (11, 12) aufweisen.

13. Sicherheits-Datenverarbeitungseinheit nach einem der Patentansprüche 1 bis 12, **dadurch gekennzeichnet, dass** der Leerfunktionsgenerator (4, 4', 4") die Leerfunktionen zufällig oder deterministisch erzeugt.

14. Verfahren zur Sicherung einer Datenverarbeitungseinheit gegen externe Lauschangriffe mit den Schritten:

    a) Erzeugen von Leerfunktionen in der Datenverarbeitungseinheit; und
    b) Ausführen der Leerfunktionen in der Datenverarbeitungseinheit.

15. Verfahren nach Patentanspruch 14, **gekennzeichnet durch** den weiteren Schritt:
    c) Kompensieren der ausgeführten Leerfunktionen in der Datenverarbeitungseinheit.

16. Verfahren nach Patentanspruch 15, **dadurch gekennzeichnet, dass** in Schritt c) Schreibvorgänge auf von Programmen nutzbare Register /Speicherstellen verhindert werden.

17. Verfahren nach Patentanspruch 16, **dadurch gekennzeichnet, dass** in Schritt c) Schreibvorgänge in der Datenverarbeitungseinheit unmittelbar verhindert werden.

18. Verfahren nach einem der Patentansprüche 16 oder 17, **dadurch gekennzeichnet, dass** in Schritt c) für Leerfunktionen Schreibvorgänge in der Datenverarbeitungseinheit auf nicht nutzbare Register/Speicherstellen (5') erfolgen.

19. Verfahren nach einem der Patentansprüche 14 bis 18, **dadurch gekennzeichnet, dass** in Schritt a) Leerbefehle erzeugt werden.

20. Verfahren nach einem der Patentansprüche 14 bis 19, **dadurch gekennzeichnet, dass** in Schritt a) zusätzliche Funktionsstufen (I - V) einer Befehlsleitung (2) aktiviert werden.

21. Verfahren nach einem der Patentansprüche 14 bis 20, **dadurch gekennzeichnet, dass** in Schritt a) zusätzliche Leer-Bus Sende/Empfangsvorgänge auf Bus-Interface Funktionsblöcke (11, 12) erzeugt werden.

22. Verfahren nach einem der Patentansprüche 14 bis 21, **dadurch gekennzeichnet, dass** in Schritt a) die Leerfunktionen zufällig oder deterministisch erzeugt werden.

FIG 1

Stand der Technik

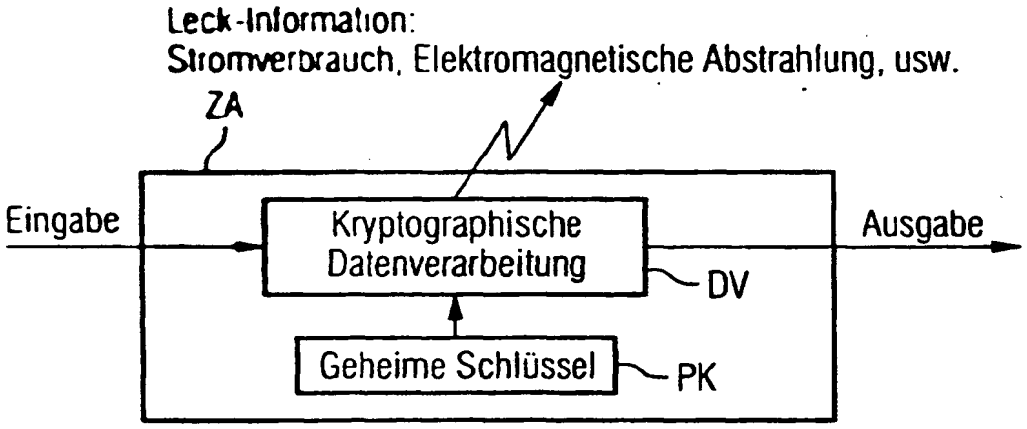
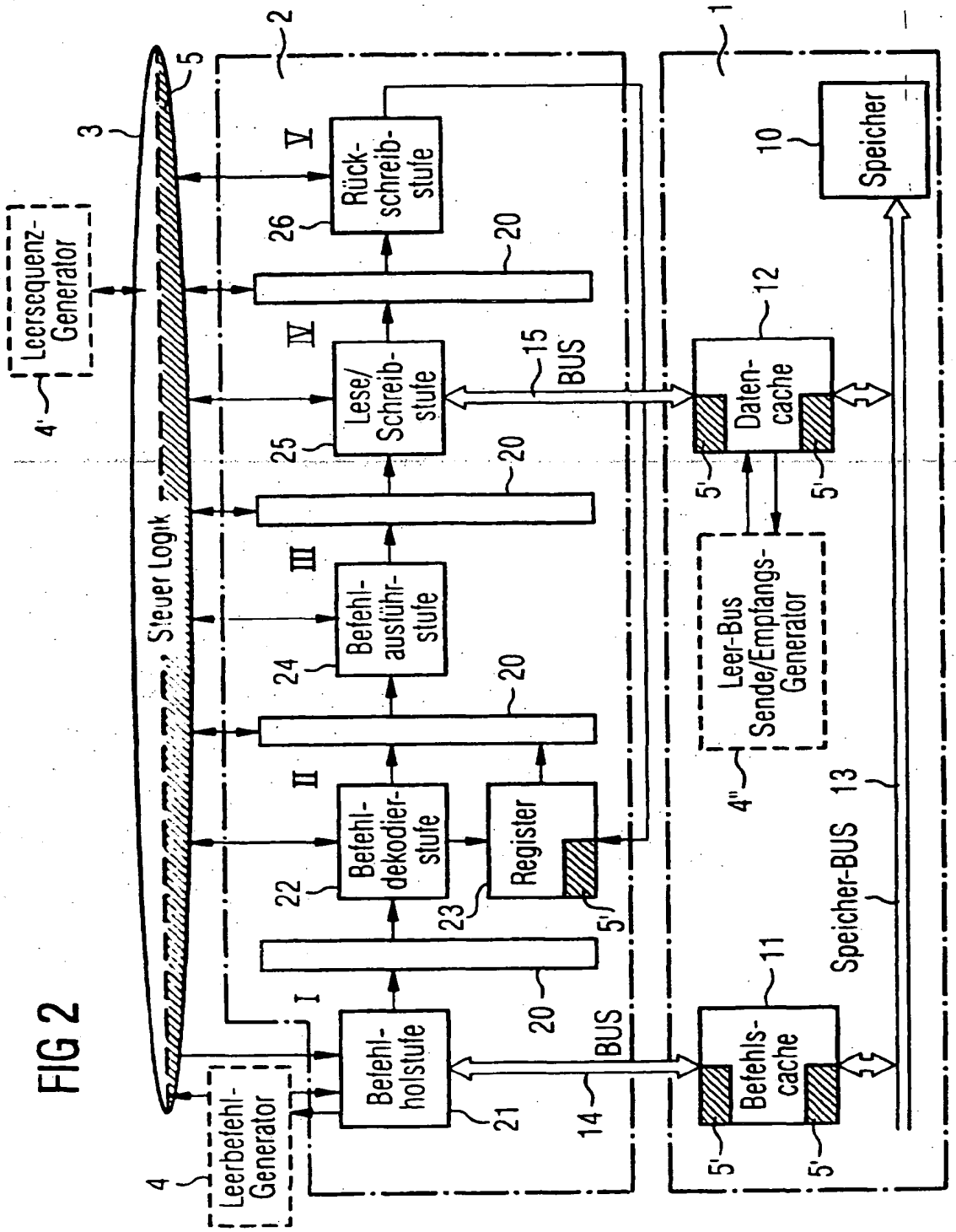


FIG 2


Steuer Logik
Leersequenz-Generator
Leerbefehl-Generator
Befehl-holstufe
Befehl-dekodier-stufe
Register
Befehl-ausführ-stufe
Lese/Schreib-stufe
Rück-schreib-stufe
Leer-Bus Sende/Empfangs-Generator
Befehls-cache
Daten-cache
Speicher
BUS
Speicher-BUS
I
II
III
IV
V
1
2
3
4
4'
4"
5
5'
10
11
12
13
14
15
20
21
22
23
24
25
26

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 11 0838

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	DE 199 36 939 A (PHILIPS CORPORATE INTELLECTUAL) 6. April 2000 (2000-04-06) * Spalte 2, Zeile 22 - Zeile 27 * * Spalte 3, Zeile 35 - Zeile 43 * * Spalte 4, Zeile 38 - Spalte 5, Zeile 9 * * Abbildungen 1-4 *	1,2,7, 14,19	G06F1/00 G06F9/38 G07F7/10
Y		8,11-13, 21,22	
Y	EP 0 404 559 A (KENDALL SQUARE RESEARCH CORP) 27. Dezember 1990 (1990-12-27) * Zusammenfassung; Abbildungen 2,3 * * Seite 2, Zeile 44 - Seite 3, Zeile 3 * * Seite 4, Zeile 55 - Zeile 57 *	8,11,12, 21	
A		1,7,14, 19	
Y	US 5 944 833 A (UGON MICHEL) 31. August 1999 (1999-08-31) * Zusammenfassung; Abbildung 1 * * Spalte 2, Zeile 26 - Zeile 31 * * Spalte 2, Zeile 35 - Zeile 42 * * Spalte 3, Zeile 51 - Zeile 58 * * Spalte 5, Zeile 20 - Zeile 60 *	13,22	RECHERCHIERTE SACHGEBIETE (Int.Cl.7) G06F G07F
A		1-3,14, 15	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	1. November 2000	Arbutina, L

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.

EP 00 11 0838

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

01-11-2000

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19936939 A	06-04-2000	WO 0019386 A	06-04-2000
		EP 1046142 A	25-10-2000
EP 0404559 A	27-12-1990	CA 2019299 A	22-12-1990
		JP 3116234 A	17-05-1991
		US 5822578 A	13-10-1998
		US 5761413 A	02-06-1998
		US 5335325 A	02-08-1994
US 5944833 A	31-08-1999	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		WO 9733217 A	12-09-1997
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.